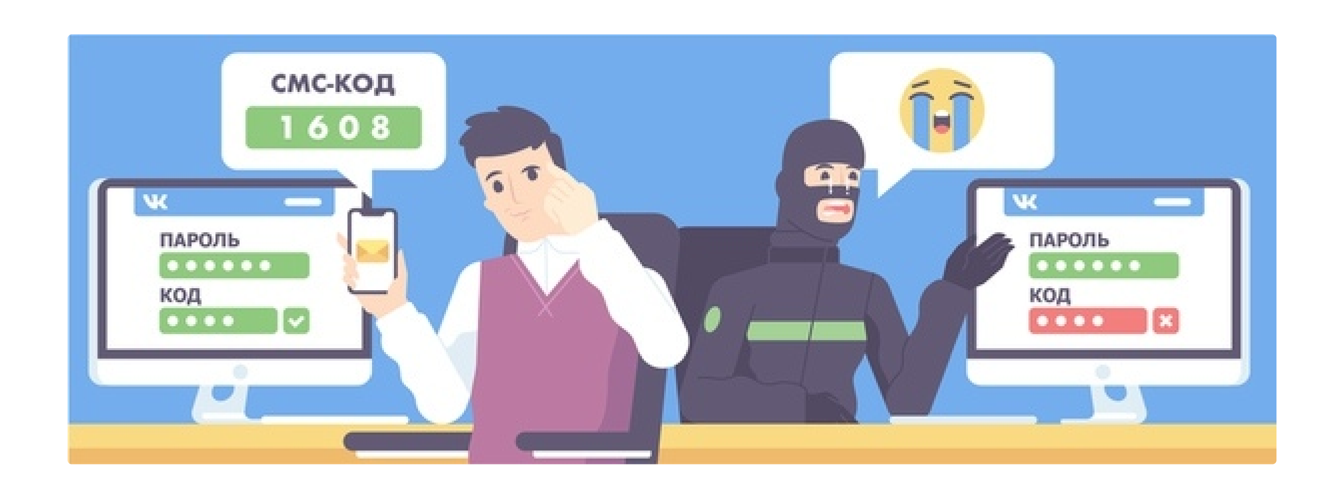
Двухфакторная аутентификация (2FA)

Надёжно защитить ваш профиль от взлома поможет функция подтверждения входа или, как её еще называют, двухфакторная аутентификация (2FA). Это очень серьёзная защита, поэтому пользоваться ею нужно вдумчиво. Делимся рекомендациями, как не потерять аккаунт, пытаясь обезопасить его от злоумышленников.



Почему она называется двухфакторной?

Потому что добавляется дополнительный уровень защиты: при входе, помимо логина и пароля, нужно ввести специальный код, полученный на привязанное мобильное устройство. Таким образом, страница оказывается защищённой двумя замками: паролем и специальным кодом. Восстановление профиля с подключённым подтверждением входа тоже становится сложнее: понадобится доступ к привязанной почте и телефону.

Если кто-то украдёт ваш пароль, попасть в аккаунт он всё равно не сможет — для этого нужно будет добраться ещё и до телефона. Чтобы сделать задачу взломщика невыполнимой, убедитесь в том, что пароли от профиля ВКонтакте и почты разные, а ваш телефон защищён паролем. Взломать аккаунт с таким уровнем защиты практически невозможно.

Как это работает?

Подключить 2FA можно в настройках: vk.com/settings?act=security в пункте «Подтверждение входа». Как только вы его подключите, в меню появится строка «Резервные коды». Это одноразовые комбинации, которые можно использовать, если у вас, например, разрядится телефон и получить код на него вы не сможете. Советуем распечатать этот список и сохранить в надёжном месте.



Теперь после ввода логина и пароля система будет запрашивать код подтверждения, который можно получить:

- личным сообщением от Администрации ВКонтакте: оно отправляется всегда, когда профиль находится в сети с какого-либо устройства;
- push-оповещением на экран привязанного смартфона;
- с помощью бесплатного SMS или звонка-сброса на привязанный номер;
- в специальном приложении для iOS (vk.cc/3SKsGl) и Android (vk.cc/2unule). Подключить его можно также через настройки безопасности.

Если получить код ни одним из этих способов невозможно, введите заранее сохранённый резервный код подтверждения.



Код подтверждения действует только **один раз**, поэтому даже если ваш логин, пароль и использованный код подсмотрят или перехватят, с их помощью всё равно не получится зайти в аккаунт снова.

После того как вы введёте код подтверждения, система запомнит ваш браузер. Это значит, что вводить в нём комбинацию в следующий раз не понадобится. Если это не ваше устройство, то перед авторизацией нужно снять галочку с пункта «Запомнить браузер».



Вы можете в любое время снять подтверждение на всех устройствах либо только на текущем. Тогда при следующей попытке авторизоваться система запросит код подтверждения повторно.

Если кто-то попытается зайти в ваш профиль, вы получите об этом оповещение:



Что важно знать перед подключением 2FA?

1. К вашему профилю должны быть привязаны актуальный email и телефон, а также загружены настоящие фотографии.
2. Если на странице нет ваших фотографий, на которых хорошо видно лицо, мы не сможем идентифицировать вас как владельца аккаунта и помочь вернуть доступ, если что-то из первого пункта пойдёт не так.
3. Если нет желания выкладывать фотографии в открытый доступ, вы всегда можете разместить их в скрытых альбомах (режим редактирования альбома: «Кто может просматривать этот альбом?» — «Только я»). Стоит также дать альбому соответствующее название, например «Это я».
   Работает только если на странице всегда были указаны настоящая фамилия и имя.

Пример правильно оформленного профиля:

Пример неправильно оформленного профиля:



При соблюдении этих простых мер (актуальный email и телефон + наличие настоящих фотографий), двухфакторная аутентификация станет надёжным щитом, оберегающим ваши данные от взлома.

Я потерял пароль от профиля, а фотографий нет. Что делать?

Если вы потеряли доступ к аккаунту с 2FA, то попробовать вернуть его можно с помощью ваших друзей. Для этого понадобится заполнить специальную форму, но сперва убедитесь, что в вашей ситуации соблюдены несколько условий:

- нужный аккаунт не заблокирован;
- вам доступен привязанный к нему номер телефона;
- вы помните фамилию, которая там была указана;
- у профиля есть 5 друзей, которых можно выбрать в качестве доверенных.

Если всё так, на экране появится предложение вернуть доступ через друзей. После вашего согласия выбранные пользователи получат коды из 6 символов.

Каждую комбинацию нужно будет ввести в произвольном порядке в специальное поле. Во время заполнения заявки вы увидите, сколько кодов уже ввели и сколько ещё осталось ввести.

Назад

Не терять логин и пароль в будущем помогут советы из нашей статьи.